

HIPAA SECURITY CHECKLIST

Administrative Safeguards

Standard	Implementation Specifications	Required or Addressable?
Security Management Process	Risk Analysis	Required
	Risk Management	Required
	Sanction Policy	Required
	Information System Activity Review	Required
Assigned Security Responsibility (Security Officer)		Required
Workforce Security	Authorization and/or Supervision	Addressable
	Workforce Clearance Procedure	Addressable
	Termination Procedures	Addressable
Information Access Management	Isolating Health Care Clearinghouse Function	Required
	Access Authorization	Addressable
	Access Establishment and Modification	Addressable
Security Awareness and Training	Security Reminders	Addressable
	Protection From Malicious Software	Addressable
	Log-in Monitoring	Addressable
	Password Management	Addressable
Security Incident Procedures	Response and Reporting	Required
Contingency Plan	Data Backup Plan	Required
	Disaster Recovery Plan	Required
	Emergency Mode Operation Plan	Required
	Testing and Revision Procedure	Addressable
	Applications and Data Criticality Analysis	Addressable
Evaluation of Security Policies		Required
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	Required

HIPAA SECURITY CHECKLIST

Physical Safeguards

Standard	Implementation Specifications	Required or Addressable?
Facility Access Controls	Contingency Operations	Addressable
	Facility Security Plan	Addressable
	Access Control and Validation Procedures	Addressable
	Maintenance Records	Addressable
Workstation Use		Required
Workstation Security		Required
Device and Media Controls	Disposal	Required
	Media Reuse	Required
	Accountability	Addressable
	Data Backup and Storage	Addressable

Technical Safeguards

Standard	Implementation Specifications	Required or Addressable?
Access Controls	Unique User Identification	Required
	Emergency Access Procedure	Required
	Automatic Logoff	Addressable
	Encryption and Decryption	Addressable
Audit Controls		Required
Integrity	Mechanism to Authenticate Electronic PHI	Addressable
Person or Entity Authentication		Required
Transmission Security	Integrity Controls	Addressable
	Encryption	Addressable